.

HIPAA
Security

Chapter 14

Access Controls

TABLE OF CONTENTS

GENERAL INFORMATION

Resources

This chapter provides a summary of the part of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requiring covered entities to implement access controls. Based on the information provided in the following documents and industry best practices, the Security Workgroup and CalOHI have developed an access control process that we believe is applicable to government business practices. The information is derived from:

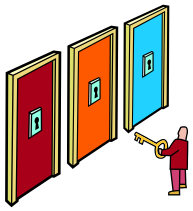
- Federal law,
- Federal regulations,
- State law,
- State regulations and guidelines,
- Federal policies and Frequently Asked Questions (FAQ),
- International Organization for Standardization (ISO/IEC),
- Project Management Book of Knowledge (PMBOK),
- Sysadmin, Audit, Network, and Security (SANS),
- National Research Council (NRC), and
- National Institute of Standards and Technology (NIST).

You will need to review the specific mandates in relation to your programs, functions, and/or business practices to determine how to apply this requirement.

Links to Resources

Links to the proposed and final federal security regulations may be found on the CalOHI Security page at CalOHI – Security. Any referenced State laws may be found on the California Law website at Find California Code or on the CalOHI Legal page at CalOHI – Legal Issues.

Decision Points



Throughout the chapter, you will find blue boxes containing decision points. Decision points target covered entities and their business associates that are required to implement the HIPAA Security Rule. Decision points identify decisions covered entities will need to make to establish their security policies and procedures.

You should review the decision points to determine which of them apply to your business practices. You may consider alternative solutions for each issue and weigh the positive and negative effects of the alternatives based on your business practices and applicable federal and State law. You may also consider your liability and the financial impact of each alternative. We strongly recommend you discuss the analysis and recommendations with your legal counsel. A sample decision tool was issued in CalOHI Policy Memorandum 2003-22 Exhibit 3. This tool may be found on the CalOHI Privacy page at CalOHI - Privacy.

We have provided checklists of the decision points and major considerations at the end of each chapter or section. You may use the checklists as guides for the decisions you need to make. Once you have established policies related to the decision points and major considerations, the policies will become part of your security policies and procedures.

Examples, Hyperlinks, and Definitions

Examples to assist in understanding the requirements are indented and printed in blue ink. Hyperlinks are provided to appropriate web site references, to pages within this chapter, and to terms posted in the CalOHI website glossary.

Standards and Implementation Specifications

The HIPAA Security Rule contains **standards**, which are requirements covered entities must meet. Within the standards, there are **implementation specifications**. Implementation specifications are more detailed activities necessary to accomplish the standard requirement. Some implementation specifications are required, and covered entities must complete these activities to be in compliance with the Rule. Other implementation specifications are addressable, which means that covered entities are required to address how they will meet the specification. Addressable implementation specifications allow covered entities more flexibility with respect to security standards compliance. It does NOT mean that the specification is optional.

For example, the unique user identification implementation specification within the access control standard requires covered entities to assign a unique name or number to workforce members who access electronic protected health information (EPHI). Covered entities should develop a process to track the unique user identities assigned to workforce members. Covered entities may decide on a particular name or number scheme for the unique user identities; if a scheme is chosen, it must uniquely identify each user who accesses EPHI.

For additional information regarding meeting addressable and required implementation specifications, see CalOHI Policy Memorandum 2004-43. It may be found on the CalOHI website at CalOHI – Security.

ACCESS CONTROL

Security Rule

The HIPAA Security Rule requires covered entities to implement technical safeguards to protect the integrity, confidentiality, and availability of EPHI. The access control standard refers to restricting access to EPHI to those individuals or groups authorized. Covered entities that implement the access control standard and its specifications will increase the security of their EPHI.

The access control standard specifically states:

"*Standard: Access Control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

The access control standard contains four implementation specifications:

- **Unique User Identification (Required). Assign a unique name and/or number for identifying and tracking user identify.** *This implementation specification will be discussed in Chapter 17, Access Authorization which may be found on the CalOHI website when released.*
- **Emergency Access Procedures (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency**.
- **Automatic Logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.**
- **Encryption and Decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.** *The encryption and decryption implementation specification will be addressed in Chapter 20: Encryption. It may be found on the CalOHI website when released.*

[45 C.F.R. § 164.312(a)(2)]

It is recommended that this chapter be used in conjunction with Chapter 17, Access Administration and Chapter 5, Workforce Security. Chapter 17 discusses unique user identification, entity authentication and authorization of access. Chapter 5 discusses the

supervision of access to EPHI, workforce clearance procedures and access termination procedures.

The goals of access control are to:

- Protect systems, resources, and data from unauthorized access, and
- Electronically ensure the appropriate level of access after an authentication procedure has been successfully completed.

EMERGENCY ACCESS PROCEDURES

Background

The HIPAA Security Rule requires covered entities to establish procedures to allow access to EPHI during an emergency. Since this is a required implementation specification, covered entities must establish emergency access procedures to satisfy this requirement. *[45 C.F.R. § 164.312(a)(1)]*

During an emergency or disaster, covered entities must remember that protecting EPHI is of utmost importance. Covered entities must have emergency access procedures for accessing necessary EPHI information. Emergency procedures may be very different from standard operating procedures, but they are necessary because the normal methods for obtaining access may fail.[1] It is important to have emergency access procedures to ensure continuity of patient care and services during emergency situations. *[45 C.F.R. § 164.312(a)(1)(d)]*

Emergencies include, but are not limited to, the following:

- **Natural disasters** – Floods, earthquakes, tornadoes, tsunamis, hurricanes, etc.,
- **Man-made disasters** – Hacking attacks, thefts, vandalism, terrorist attacks, etc., and
- **Unforeseen disasters** – Power outages, internal failures, etc.

Covered entities may already have emergency access procedures in place (e.g., as part of their contingency plans). These plans may or may not address EPHI access. You will need to ensure your emergency access procedures address EPHI access if they do not already.

Contingency Planning

The HIPAA Security Rule's contingency plan standard requires covered entities to establish policies and procedures to respond to emergency disasters (e.g., power outages, earthquakes, floods, etc.) that may potentially damage the systems that contain EPHI.

Under the contingency plan standard, covered entities are required to develop disaster recovery plans. The goal of disaster recovery is to minimize a disaster's effects. This can be achieved by taking the necessary steps to ensure that a covered entity's resources,

[1] TMA Privacy Office Information Paper, HIPAA Security: Access Controls, TMA Privacy Office, http://www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity/images/pdf/Access%20Contr.%20HSIP22.pdf, November 2003

personnel, and business processes resume operation in a timely manner. Covered entities must ensure their disaster recovery plans explicitly include EPHI.

For more information regarding contingency planning and disaster recovery, see Policy Memorandum 2005-62, Chapter 11: Contingency Planning. It may be found on the CalOHI website at CalOHI – Security.

STATE REQUIREMENTS

State rules require State departments to have an operational recovery plan, which provides the necessary preparation to design and document a sufficient set of procedures to ensure continued agency operations in the event of a disaster or any other event resulting in unplanned discontinuation of IT systems operations. *[SAM § 4843]*

DECISION POINT: Current Emergency Access Procedures

Does your department have emergency access procedures? Do they include access to EPHI?

You need to determine if your organization already has emergency access procedures. If not, you will need to develop these procedures. If your organization already has emergency access procedures, you must determine if they address EPHI access. If not, you will need to modify your emergency access procedures to include EPHI access. You will need to document this decision as part of your security policies and procedures.

Emergency Access Procedures

The following is a 10-step emergency access process a covered entity may implement to control EPHI access during an emergency.

1. **Declaring an Emergency** – Determine how the covered entity will declare an emergency. When an emergency occurs, the covered entity's management (e.g. Director, Information Security Officer (ISO), etc.) should declare that the business has been adversely affected by an event (e.g. bioterrorism, earthquake, flood, etc.). This usually will mean that business cannot continue without some form of contingency operations.

2. **Determining Emergency Responsibility** – Determine who will be responsible for managing all subsequent emergency access procedure responsibilities. This designation should be documented.
3. **Determining Who Needs Access** – Determine who will need emergency EPHI access. Some people who will need emergency EPHI access may include managers (e.g., Privacy and Security Officers, Chief Information Officer (CIO), etc.). If you provide health care services, physicians and other health care providers may also need access. Workforce members requesting emergency EPHI access may be required to obtain approval from their manager first.

   For more information regarding disaster recovery and emergency mode operations, see Chapter 11: Contingency Planning. It may be found on the CalOHI website at CalOHI – Security.

DECISION POINT: Determining Who Needs Emergency Access

Who will need access to EPHI during an emergency?

You will need to determine which workforce members need emergency EPHI access. This decision may be based upon your business practices. Covered entities will most likely grant access to the Privacy Officer, Security Officer, and CIO. Workforce members who wish to receive emergency EPHI access must follow the required steps for obtaining emergency EPHI access, which may involve a request form or verbal acknowledgement from the identified individual who approves access during emergencies.

MAJOR CONSIDERATION: Pre-approved Access

You should consider implementing a pre-approved staff list of workforce members that will have access to EPHI during an emergency. By doing this, covered entities can prepare for emergencies beforehand and save valuable time by not having workforce members wait for approval during an emergency. Preparing a pre-approved list will reduce the amount of effort to determine who will need access during an emergency. However, as with any planning actions, the pre-approved list must be continually updated to reflect changes in your workforce. If you decide to implement a pre-approved staff list, you must document this as part of your security policies and procedures and update it as staffing changes.

DECISION POINT: Providing Emergency Access to EPHI

Who will provide access to EPHI during an emergency?

Providing emergency access should NOT be the responsibility of the Privacy or Security Officer. Appointing someone else to provide emergency access establishes a separation of duties. The individual who will provide EPHI access during an emergency should be a designated member of the emergency mode operations team who is responsible for security and recovery procedures (e.g., IT system administrator, *see Chapter 11: Contingency Plan for more information about emergency operations mode*). You must document this decision as part of your security policies and procedures.

4. **Determining Necessary Access** – Since EPHI information may not be secured during an emergency, covered entities should not grant access to all workforce members who previously had access to EPHI. Covered entities should grant access to only those workforce members who need access during an emergency. Workforce members who request emergency EPHI access must state the reasons why they will need access on the request form. Some reasons may include:
   - Patient care activities, and/or
   - Access to EPHI is necessary to establish access for others requiring it.

5. **Completing Request Forms** – Anybody who requests EPHI access must fill out an access request form or gain verbal approval from the identified individual who approves access during emergencies. *Refer to Exhibit 2 for a sample request form which may be customized to reflect a covered entity's business practices.* At a minimum, the request form should require the individual to fill out his/her name, his/her title or position, date of request, duration of access, and the reason(s) for needed emergency access. Security best practices recommend that covered entities require request forms and keep copies or keep a record log of all workforce members given verbal emergency EPHI access.

6. **Receiving Manager Approval** – After the individual finishes filling out the request form, he/she must turn this form into his/her manager for the next level of approval, when appropriate. The manager must determine if he/she will approve the individual's emergency EPHI access request. If the manager decides to approve the access request, he/she will need to indicate his/her approval by signing on the form. In addition, the manager must determine the level of access the requestor will have based on the request form reason(s). The requestor's role and responsibilities should also be considered when determining the level of access. The manager will need to record the level of access on the form.

7. **Forwarding Form to the Privacy or Security Officer** – After the manager approves access and determines the amount of access for the individual, he/she will need to forward the form to the Privacy or Security Officer. One of the officers must sign the form if he/she agrees with the manager's approved access and the level of access.

8. **Submitting Form to Approval Administrator** – The Security or Privacy Officer will then submit the request form to the approval administrator responsible for providing emergency access (e.g., IT system administrator) so that he/she can activate a username and password for the individual.

9. **Activating Username and Password** – The IT system administrator will activate a username, password, and level of access for the workforce member. He/she will then need to document the request and activation of the username, password, and level of access. In addition, the IT system administrator may make copies of the request form to keep on file.

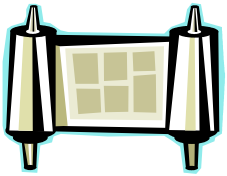
10. **Sending Account to Workforce Member** – The IT system administrator will send back the form to the individual with the activated username and password. The IT system administrator should notify the manager, Privacy Officer, and Security Officer of the account activation.

Depending on the scale of the emergency, covered entities may modify the above process by adding, modifying, and/or removing steps.

Resuming Operations

Management will determine when the disaster is over and when to resume standard operations. At that time, the emergency mode operations team must ensure that ordinary access to EPHI has been restored and that users are able to log in normally. Emergency access privileges must be terminated when operations return to normal.

Documentation



It is important to document all steps of the emergency access process, from the declaration to the aftermath of the emergency. Should an emergency situation arise again, documentation of prior emergency situations and procedures will be an important reference tool. Documentation should be provided to any auditors who request the information.

Planning for emergency access should be included in an organization's contingency plan.

DECISION POINT: Contingency Plan

Have you included emergency access procedures in your contingency, disaster recovery, and emergency mode operations plans?

You must include emergency access procedures in your contingency plans. You must inform the Disaster Recovery Director, Disaster Recovery Team, Privacy Officer, Security Officer, and others who will be involved with this process during an emergency.

AUTOMATIC LOGOFF

Background

Automatic logoff is an addressable implementation specification under the Security Rule's access controls standard. *[45 C.F.R. § 164.312(a)(2)(iii)]* Automatic logoff is defined as implementing electronic procedures that terminate an electronic session after a predetermined time of inactivity. Covered entities must address this implementation specification by implementing automatic logoff, if available. If the EPHI application does not have automatic logoff ability, the covered entity must implement an alternate solution that accomplishes the same goal. The covered entity must document how this alternate solution meets the intent of automatic logoff.

Automatic logoff is a security control that prevents unauthorized individuals from accessing EPHI. When a workstation that accesses EPHI is left unattended, unauthorized individuals can access the workstation and have the ability to view, copy, edit, and/or delete EPHI. Automatic logoff reduces the probability of unauthorized individuals accessing unattended workstations that contain EPHI. Ultimately, the goal of implementing automatic logoff is to ensure only authorized users are accessing and using EPHI.[2]

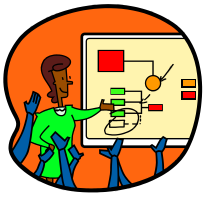
When the workforce accesses the application again, the automatic logoff feature requires re-authentication. Automatic logoff will not log the user out of all running applications, only the applications that have automatic logoff enabled.

For example, a user has a word processor application, Internet browser, and EPHI application running on his/her workstation. Automatic logoff will log the user off the EPHI application after a certain period (e.g., 15 minutes) of inactivity and will not affect the word processor application or Internet browser (i.e., these two applications are left running).

---

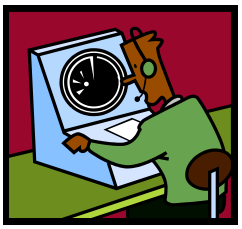
[2] Haber, Wayne, *Automatic Logoff: GIAC HIPAA Security Certificate (GHSC) Practical Assignment – Version 1.1*, SANS Institute 2004, Automatic Logoff, June 2004.

Risk Analysis Results



Covered entities should review their risk analysis results to determine if workstations that access, transmit, receive, or store EPHI are at risk for unauthorized access. The HIPAA Security Rule requires covered entities to perform a risk analysis as part of their security management process. Servers, workstations, or other computer systems located in open, common, or otherwise unsecured areas should enable both automatic logoff mechanisms and password protected screensavers after a predetermined amount of inactivity.

Automatic Logoff Feature



Applications and/or workstations that access, store, receive, and transmit EPHI may have automatic logoff capability. Covered entities should verify if their systems have this capability. This can be determined by asking the users who support the EPHI application or through system documentation. If the EPHI application is a commercial-off-the-shelf system, covered entities may contact their vendor to determine if the application has the ability to automatically logoff.

> For example, Mike contacts his systems programmer to determine if the EPHI application he is working with has automatic logoff capability. The system programmer does not know, and there is no documentation on the subject. Mike contacts the EPHI application vendor and determines that automatic logoff is a feature that can be enabled on the application.

DECISION POINT: Automatic Logoff

Do your applications and/or workstations that access, store, receive, and transmit EPHI have automatic logoff mechanisms that logoff the user after a predetermined amount of inactivity?

You will need to determine if your applications and/or workstations that contain EPHI already have automatic logoff enabled as a security feature. You will need to document this determination as part of your security policies and procedures.

State Requirements

The State Administrative Manual (SAM) does not mention automatic logoff specifically but states that a State department must protect and ensure the integrity of its EPHI. SAM states:

State agencies need to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure the physical security of these resources. State agency heads are accountable for the computerized information resources held by their agencies. They are responsible for the integrity of computerized information resources, and the authorization of access to those resources. All agency employees share in this responsibility as well. *[SAM § 4840]*

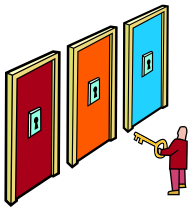
Although SAM does not specifically require a State department to implement automatic logoff, this security measure must still be implemented as part of HIPAA's requirement on protecting EPHI integrity.

Predetermined Amount of Inactivity

Before implementing automatic logoff, covered entities will need to determine a reasonable and appropriate time of inactivity before the application logs off the user and a password protected screensaver or equivalent security measure is enabled. This period of time will be determined by a covered entity's business practices.

The amount of time should ensure EPHI is properly protected on workstations but should not inconvenience users. If the period of inactivity is too short, and the application automatically logs users off too soon, workforce members will become frustrated, and productivity will be lost. If the period of inactivity is too long before the application automatically logs off users, then unauthorized users may have sufficient time to view and modify EPHI.

For example, billers at a clinic were unhappy that their automatic logoff time was originally set to 15 minutes. Since it often took 20 minutes to finish filing their paperwork, automatic logoff was set too soon for their business needs. When they returned to their workstations, they found that their session ended, and they would need to log back in again, thus wasting time. In the end, they requested to increase the logoff time to 30 minutes instead of 15 minutes.



DECISION POINT: Predetermined Amount of Inactivity

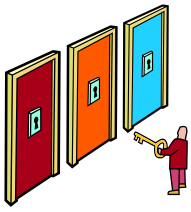
What is a reasonable and appropriate time of inactivity before automatic logoff, password protected screensavers, or equivalent security measures are enabled?

You will need to determine a reasonable and appropriate time of inactivity before your automatic logoff security measures are enabled. You will need to consider your business practices to determine this time. You will need to document this decision as part of your security policies and procedures.

Varying Timeouts Accordingly

Workforce members may find logging onto a workstation every time they leave it unattended to be a frustrating and time-consuming process. A covered entity may choose to vary timeouts according to job position or workstation location to reduce workforce members' frustrations. Workstations in locations with little unauthorized traffic probably do not need the short logoff time required in more exposed areas.[3]

Workforce members who constantly access EPHI will most likely need a longer period before logoff compared to those members who do not access EPHI as frequently. Workforce members who spend a lot of time gathering information and whose computers become inactive because of that may need a longer period before timeout.



DECISION POINT: Varying Timeouts Accordingly

Will you vary your timeouts accordingly?

You will need to determine if it is necessary to vary timeouts according to job function or workstation location. If you decide to vary your timeouts, this decision must become part of your security policies and procedures documentation.

---

[3] HIPAAdvisory, No. 46 HIPAAtech: *To Logoff or Not to Logoff -- That is the Question*, Phoenix Health Systems, http://www.hipaadvisory.com/action/Notes/vol1/oct.htm, October 2001.

Security Best Practices

Security best practices indicate covered entities enable both automatic logoff and password protected screensavers after a predetermined amount of inactivity. This will offer more EPHI protection as well as more than satisfy the addressable implementation specification. If you decide to implement both, this must be documented as part of your security policies and procedures.

Residual Risk

Implementing automatic logoff security measures will help protect the confidentiality and integrity of EPHI. However, risks still exist even after automatic logoff security measures have been implemented.

> For example, an unauthorized user may access a workstation before automatic logoff and/or password protected screensavers have been enabled. Within those first 15 minutes (or whatever time period a covered entity chooses to be the amount of inactivity before logoff), an unauthorized user can view and/or edit EPHI because automatic logoff security measures have not yet been activated.

To mitigate this residual risk, a covered entity may choose to decrease the amount of time before logoff, but this may cause inconvenience to workforce members. Another option is to train workforce members to lock their workstations prior to leaving them unattended. A covered entity must determine and document a reasonable balance between addressing the residual risk and inconveniencing workforce members and thus, productivity.

Alternative Solutions

If a covered entity's EPHI application does not have automatic logoff capability, another security measure that performs the same function must be implemented to satisfy the addressable implementation specification.

An alternative would be to implement password protected screensavers. A password protected screensaver is a feature that locks the screen and is enabled after a predetermined amount of inactivity. Since password protected screensavers lock the screen, this security measure will help prevent unauthorized users from accessing an unattended workstation. If a workforce member returns to his/her workstation and wants to unlock the screen, a password must be entered to unlock the workstation for use.

Other preventative measures may include:

- Requiring workforce members to logoff their computer every time they leave their workstation. This may be accomplished through policies and procedures enforced by sanctions, or
- For small offices, keeping computers that contain EPHI in a room that must be locked whenever workforce members leave their workstation.

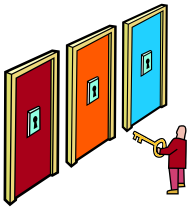
Workstation Screen Lock

If workstations have a screen lock feature available, security best practices recommend that workforce members enable this feature every time they leave their workstation unattended. This will help prevent unauthorized individuals from accessing unattended workstations.

> For example, many systems, pressing "Ctrl + Alt + Delete" simultaneously will enable a menu where one of the choices is to "Lock computer." Choosing this command will lock your computer, and workforce members will have to re-enter their passwords to access their workstations.

For more information regarding workstation use, see Chapters 6 & 7: Workstation Use and Workstation Security, which CalOHI will release in the spring of 2005. When released, it may be found on the CalOHI website at CalOHI – Security.

Training Workforce Members



Covered entities will need to train their employees to ensure that they understand the policies and procedures concerning automatic logoff or the alternative implemented.

DECISION POINT: Training Workforce Members

Have you trained your workforce members on automatic logoff policies and procedures?

You will need to train your members on the use of automatic logoff security measures, whether you choose to implement automatic logoff, password protected screensavers, and/or some other equivalent security feature. You also need to document this training as part of your security policies and procedures.

DECISION POINTS

ISSUE IMPACTS	DATE STARTED	PERCENT COMPLETED	DATE COMPLETED	ITEM DESCRIPTION
☐				Current Emergency Access Procedures
☐				Determining Who Needs Emergency Access
☐				Providing Emergency Access to EPHI
☐				Contingency Plan
☐				Automatic Logoff
☐				Predetermined Amount of Inactivity
☐				Varying Timeouts Accordingly
☐				Training Workforce Members

MAJOR CONSIDERATIONS

ISSUE IIMPACTS	DATE STARTED	PERCENT COMPLETED	DATE COMPLETED	ITEM DESCRIPTION
☐				Sharing Credentials
☐				Pre-approved Access

REFERENCES/WORKS CITED

The following references are provided for your use as needed. CalOHI does not endorse any of the following resources, but simply provides them as potential sources for your enhanced knowledge.

State Administrative Manual (SAM)

The State Administrative Manual is a reference source for statewide policies, procedures, regulations, and information developed and issued by authoring agencies.

State Administrative Manual Sections:
4843 – Operational Recovery Planning
4840 – Security and Risk Management
4841.2 – Information Integrity and Security
4842.2 – Risk Management

SANS Institute

A Consumer Guide for Personal File and Disk Encryption Programs, Baldwin, Scott, http://www.sans.org/rr/whitepapers/vpns/884.php

Automatic Logoff: GIAC HIPAA Security Certificate (GHSC) Practical Assignment –Version 1.1, Haber, Wayne, June 2004. Automatic Logoff.

Disaster Recovery Plan Strategies and Processes, Feb 2002. http://www.sans.org/rr/whitepapers/recovery/564.php

Plugging the Holes, Your Data is Leaking Out, Downey, Robert, http://www.sans.org/rr/whitepapers/basics/422.php

The Disaster Recovery Plan, June 2003. http://www.sans.org/rr/whitepapers/recovery/1164.php

---

Other Resources

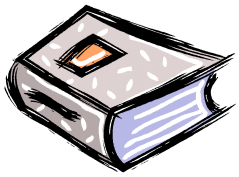
Computerworld, Data Thefts Prompting IT Security Checks, Mearian, Lucas, March 21, 2005, http://www.computerworld.com/hardwaretopics/storage/story/0,10801,100491,00.html

HIPAAdvisory, To Logoff or Not to Logoff - That is the Question, Oct 2001. http://www.hipaadvisory.com/action/Notes/vol1/oct.htm

TMA Privacy Office, HIPAA Security: Access Controls, Nov 2003, http://www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity/images/pdf/Access%20Contr.%20HSIP22.pdf.

Windows Security, Securing Your Pocket PC, Shinder, Deb, http://www.windowsecurity.com/pages/article_p.asp?id=1344

National Institute of Standards and Technology (NIST)



NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005, http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

NIST Special Publication 800-63, Electronic Authentication Guideline , September 2004, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

---